

TLP: AMBER

WARNING: Information in this report is FOUO//TLP: AMBER. Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information. Recipients may only share this information within their own government organization, and only as necessary to act on that information, consistent with both the DHS policy relating to FOUO information and with the Traffic Light Protocol, <http://www.us-cert.gov/tlp>.

ACTIONS

A TTX is scheduled for the afternoon of November 1, to test federal communications and coordination processes and resolve any technical or coordination challenges ahead of Election Day.

Continue to work leads to find points of contact within the Trump Campaign.

(b) (5), (b) (7)(E)

INCIDENT SUMMARY

| | |
|--|-----------|
| States Reporting Successful Intrusion | 3 |
| States reporting election related incidents with infrastructure match to open FBI investigation | 11 |
| States reporting election related incidents with non-matching infrastructure to open FBI investigations | 6 |
| Total States reporting election related incidents with infrastructure match to FBI investigations | 20 |
| Third party vendors reporting successful election related intrusions | 2 |
| Third party vendors reporting election related incidents with matching infrastructure to open FBI investigations | 1 |
| Total third party vendors reporting election related incidents | 3 |
| States reporting non-election / inconsequential incidents | 2 |

STATE VULNERABILITY SCANNING & ASSESSMENTS

| | |
|---|-----------|
| NCCIC & SECIR Outreach, Testing, and Scanning – Election Status | |
| State Level Cyber Hygiene / RVA Outreach/Inquiries (All states expect: (b) (7)) | 48 |
| Local Level Inquiries | 35 |
| State Level Cyber Hygiene Scanning in Progress | 25 |
| Local Level Cyber Hygiene Scanning in Progress | 24 |
| Private Cyber Hygiene Scanning in Progress | 1 |
| State Level RVA Assessment in Progress - (b) (7) | 1 |
| Total Testing/Scans in Progress | 51 |

MEETING

Daily Election Infrastructure Call (b) (6), EPMO)

Meeting designed to sync election outreach efforts across NPPD.

Monday | Wednesday | Friday, 0830-0900, Teleconference (FO, I&A, OLA, OGC, IGA, PLCY, S&T, NCATS, SECIR, IP, OCIA, OPA)

Daily Election Sync (b) (6), NCCIC)

General sync call between NCCIC, FBI and CTIIC for information sharing purposes.

Daily, 1030-1100, Teleconference (FBI MM, CYWATCH, CTIIC, MS-ISAC)

UCG Seniors Call

Monday | Wednesday | Friday, 1200, Teleconference (DHS, FBI, CTIIC)

UNCLASSIFIED//FOUO
Election Related State Incidents

| | |
|---|-----------|
| States Reporting Successful Intrusion (a) | 3 |
| States reporting election related incidents with infrastructure match to open FBI investigation (b) | 11 |
| States reporting election related incidents with non-matching infrastructure to open FBI investigations (c) | 6 |
| Total States reporting election related incidents with infrastructure match to FBI investigations (a+b+c) | 20 |
| Third party vendors reporting successful election related intrusions (d): | 2 |
| Third party vendors reporting election related incidents with matching infrastructure to open FBI investigations (e): | 1 |
| Total third party vendors reporting election related incidents (d+e) | 3 |
| States reporting non-election / inconsequential incidents (d) | 2 |

States Reporting Successful Intrusion (a)

| State | Date of Activity | Description | Status | Source | Intrusion | Exfil | Owner |
|-------|------------------|---------------------|--------|--------|-----------|-------|-------|
| █ | █ | (b) (5), (b) (7)(E) | █ | █ | █ | █ | █ |
| █ | █ | █ | █ | █ | █ | █ | █ |
| █ | █ | █ | █ | █ | █ | █ | █ |

Third party vendors reporting successful election related intrusions (d):

| State | Date of Activity | Description | Status | Source | Intrusion | Exfil | Owner |
|-------|------------------|---------------------|------------|--------|-----------|-------|-------|
| █ | █ | (b) (5), (b) (7)(E) | █ | █ | █ | █ | █ |
| - | | | CLASSIFIED | | | | |

UNCLASSIFIED//FOUO

States reporting election related incidents with infrastructure match to open FBI investigation (b)

| State | Date of Activity | Description | Status | Source | Intrusion | Exfil | Owner |
|------------|------------------|---------------------|------------|------------|------------|------------|------------|
| [REDACTED] | [REDACTED] | (b) (5), (b) (7)(E) | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| - | | | CLASSIFIED | | | | |
| [REDACTED] | [REDACTED] | (b) (5), (b) (7)(E) | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |

UNCLASSIFIED//FOUO

Third party vendors reporting election related incidents with matching infrastructure to open FBI investigations (e)

| State | Date of Activity | Description | Status | Source | Intrusion | Exfil | Owner |
|-------|------------------|---------------------|--------|--------|-----------|-------|-------|
| █ | █ | (b) (5), (b) (7)(E) | █ | █ | █ | █ | █ |

States reporting election related incidents with non-matching infrastructure to open FBI investigations (c)

| State | Date of Activity | Description | Status | Source | Intrusion | Exfil | Owner |
|-------|------------------|---------------------|--------|--------|-----------|-------|-------|
| █ | █ | (b) (5), (b) (7)(E) | █ | █ | █ | █ | █ |
| █ | █ | █ | █ | █ | █ | █ | █ |
| █ | █ | █ | █ | █ | █ | █ | █ |
| █ | █ | █ | █ | █ | █ | █ | █ |
| █ | █ | █ | █ | █ | █ | █ | █ |
| █ | █ | █ | █ | █ | █ | █ | █ |

States reporting non-election / inconsequential incidents (d)

| State | Date of Activity | Description | Status | Source | Intrusion | Exfil | Owner |
|------------|------------------|-----------------------------------|------------|------------|------------|------------|------------|
| [REDACTED] | [REDACTED] | (b) (5), (b) (7)(E) [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |

| MS-ISAC ALBERT sensor detecting net flow interactions (NFI) with infrastructure related to FBI investigations | |
|---|------------|
| (b) (5), (b) (7)(E) [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |